I CLAIM:

1. A system for detection and blocking of IP collisions, comprising:

a communication interface and communication kernel module that provides a communication interface that enables a collided IP detection system to share information with other hosts and provides a kernel for controlling the communication;

a network interface driver module that is connected with a physical device that is a network interface and an upper communication module to transmit packets to the network, and transmits packets collected in the network to the upper communication module;

a network interface module that is connected to the devices connected to the network;

a packet capture driver module that collects all packets detected in the network;

an ARP packet filtering module that filters only ARP packets among the packets being captured from the packet capture driver module;

an IP collision decision module that determines if the collected packets are collided IP packets and, if so, transmits the results to a listing module;

an access blocking decision module that notifies an access status if an ARP request packet is included in an access blocking policy list;

an access blocking module that, depending on the access blocking decision module's decision to block the access on a particular packet, blocks the network access by transmitting an ARP respond packet to the blocked packet;

a data storage module that stores information set to operate the collided IP detection system, a detected collided IP list, and a newly detected host's IP and MAC address lists;

a search list logging and saving module that internally lists the detected collided IP data and periodically it saves in a storage medium; and

a detection result notification module that transmits the detected collided IP data to another system and notifies the administrator of it,

wherein when the ARP packet is collected from the network, each ARP packet is classified into a request packet and a respond packet after being identified, and then if it is a new request packet, it is added to the list, but if it is a respond packet that also exists in input request ARP packet list, the packet's collision is detected and at the same time the ARP packet's access is blocked.

2. A method of detecting IP collisions using an IP collision detection system between a client and a server, comprising the steps of:

collecting all packets created by accessing the network;

filtering only ARP packets among the collected packets;

determining whether the filtered ARP packet is an ARP request packet or an ARP respond packet;

adding a MAC address to a list by IP address if the filtered ARP packet is an ARP request packet;

incrementing a count by one each time if the filtered ARP packet is an ARP respond packet;

determining if the number of the ARP respond packets occurring by IP exceeds the frequency set within a predefined time out period, and if it exceeds the set frequency, confirming it as IP collision and adding it to the list; and

if the number of the ARP respond packets occurring are less than the set frequency, resetting each IP's counter.

3. A method of blocking collided IP using an IP collision blocking system between a client and a server, comprising the steps of:

collecting all packets transmitted over a network;

filtering only ARP packets among the collected packets;

determining whether the filtered ARP packet is an ARP request packet or an ARP respond packet;

confirming if an IP address and IP or MAC are included in a block policy list if the filtered packet is an ARP request packet;

unicasting the ARP respond packet to block access to a corresponding host if an ARP request packet is included in the policy list; and

broadcasting the ARP respond packet to block access after unicasting the ARP respond packet, thereby blocking the network access.